Copy Protection of Computer Games

Richard Hyams

Technical Report
RHUL-MA-2008-03
15 January 2008

Department of Mathematics
Roal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

COPY PROTECTION OF COMPUTER GAMES

Author: Richard Hyams

Supervisor: Dr Peter Wild

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In this dissertation we look at the effectiveness of copy protection for computer games distributed on physical media such as CD and digitally, over the internet. To set the scene a history of computer game piracy is described and the threats to today's computer games in terms of piracy are reviewed. A demonstration of how to obtain a pirated game is performed to show how easy this has become since the growth of the internet. Copy protection techniques are then described initially from an historical perspective and then by looking at the state of the art for both physical media and online distributed copy prevention. Each is reviewed by looking at the capabilities and shortcomings along with the possible methods of attacking each type of protection. We find that at present with the new techniques that online distribution bring that it is far more effective than physical media protection. The technique of making the consumer bind their game to an account which allows them to play online has been particularly effective. Finally it is demonstrated that online copy protection is effective in the real world, by investigating how long it takes for a copy protection to be bypassed for a number of computer games released either on physical media or online. It was found that none of the games released online had any pirated copies available online leading to the conclusion that this protection had not been bypasses yet. It was however noted that most of the computer game titles with large sales were released both online and on physical media and therefore the attack will be towards the physical media copy protection rather than online and so until games are only distributed online can we be really totally sure of the online copy protection effectiveness.

1. Introduction

Copy protection historically was concerned with preventing users from making copies of computer games on physical media such as CD, DVD or game consoles disks. As the computer games industry grows and uses other methods of distribution through the internet interest in copy protection has grow [BC04]

The widespread acceptance of the Internet and the huge advances in computers has made possible the distribution of assets in a digital format far cheaper than ever before. Large hard disk drives and physical media writers are now the norm and so copying a computer game is a matter of copying the bytes to the storage medium. Distributing of copied digital assets can be done illegally by sharing it with an online community without any payment to the copyright holder.

According to the business software alliance [BA06] in 2006 $40 billion worth of illegal software was installed on computers globally. Looking just at computer game in the US , sales in 2006 reached $7.4 billion [ES06] whilst it is estimated that the industry lost more than $1.9 billion to global piracy [II07] As Piracy rates increase the games industry is increasingly interested in mechanisms for preventing piracy.

This dissertation is concerned with looking at the threats to computer game by examining why computer games are pirated and the threats against them. A case study will be used to show how a pirated computer game can be obtained. A review of copy protection schemes is then undertaken along with the techniques and tools available to break them. A case study investigating games released by Eidos Interactive will investigate how quick a pirated game is available for both physical media and online release games.

Digital rights management (DRM) is often seen as a method of copy protection but copy protection is now just one part of what is known as DRM. Renato [RI01] suggests although DRM was originally conceived to help with the copy protection of digital content it now involves all aspects of digital distribution, ranging from not just preventing copying but to content metering to payment processes and audit records This dissertation will confine itself

to discussing the copy protection aspects of DRM and how they relate to digital computer game assets

Copy protection of computer games is very important for protecting sales it is not needed for the entire life that a game is sold. The majority of sales occur in the first 6-8 weeks of release so the main goal of copy protection is to protect the game during this period. Copy protection after this period and hence cracks will have a decreasing affect on sales numbers. However it is necessary to look at the secondary games market. This is basically a second-hand market for computer games where pre-played games. Many computer game retail stores have set up facilities to buy back the game for resale. The game developers and publishers do not receive any sales from this market but will have a downward pressure applied on prices of the new full-priced games as soon as the game appears on the secondary market. Copy protection which links a copy to a user or a device would certainly depress the affects of the secondary market.

Through out this dissertation a variety of terms will be used. The term computer game refers to games that can be played on a PC. A game sold on physical media is a game sold on a CD or DVD by a retail outlet whereas an online game is distributed online by downloading from an internet site. A pirated computer game is a computer game with its copy protection removed The term hackers is used to refer to people involved in removing copy protection and software privacy is the illegal copying and distribution of computer game software purchased by someone else. The term crack will be used to define a game executable on which the copy protection mechanism has been removed.

Although computer game industry spans not just personal computer (PC) games but also games for consoles such as the Sony Playstation and Microsoft Xbox online distribution has only just started to take off for consoles and has been around longer for PC games so this dissertation will concentrate on PC games rather than consoles.

2. A history of computer game piracy

Bruce sterling [BS92] gives a good overview on the history of computer game pirating or cracking as it is commonly known. Piracy started way back in the late seventies with the APPLE II users sharing software. By the early eighties some machines such as the BBC micro were being targeted by so many hacker groups that many software companies gave up producing software because of the lack of profits being made.

With the advent of the first community bulletin board systems it became possible to exchange pirated copies of games, cracks or just instructions on how to crack the latest game releases. Bulletin boards (BBS) however cost money to run and so special paying accounts were setup for people not in the pirate community to have access to cracked software. BBS operators however were running big risks as unlike web sites the BBS were based at the system operator's home and could be traced by the police. For this reason the scene was very secretive and underground with phone numbers and names traded between people that knew each other and even voting on by existing members of a BBS .Microsoft, Novell and other large corporations became so concerned that they worked with the FBI to try and close the BBS down. In 1997 Operation Cyberstrike [BS92], run by FBI's international computer crime department in san Francisco shutdown 5 major pirated BBS in one week and caused many others to shutdown in fear., Some authors [BS92,BG04] point out that this probably began the push of the whole pirate community onto the internet. New methods of pirating over the internet started with using IRC channels which then evolved into Peer to peer networks (P2P)

A person trying to find pirated games use to have to go through the difficult process of hunting down a BBS or FTP site and obtain a password and then possibly apply for membership however now with the emergence of the internet once what was relative hard has become a lot easier.

3. Threats to Computer game

This section will look at the threats to computer to help understand why piracy has taken place in the past and why it is still continuing.

3.1 Consumers

One of the biggest challenges facing games publishers and developers is the consumers' indifference to copy protection rights. Although using pirated software could be seen as similar to shoplifting consumers seem to be accepting of using pirated computer games

Macrovision [MA07] conducted a survey on a number of popular gaming sites. Of the 2,219 respondents 52% admitted to acquiring cracked versions or using pirated software. It should be noted that Macrovision is the world's largest maker of copy protection software so it may be in their interest to make piracy seem worse than it really is.

A further survey looking at consumers and counterfeited was conducted by Bryce and Rutter for the organised crime task force of Northern Ireland and found 15% of 2000 people had downloaded copied computer games and [JB04] .It must be noted that compared with the Macrovision survey which was conducted with computer game players, Bryce and Ratter's survey was a sample of the general population. This survey found that the main reason for consumers to use pirate computer game is because they are cheaper than the original computer game copy.

Another route consumers can obtain pirate is through casual game copying. A computer game with poor or no copy protection runs the risk of the consumer making a pirate copy for a friend or a small number of friends often free of charge. This is basically just making a direct copy of the game using a DVD\CD recorder drive. These consumers involved in casual game copying are not hackers and generally only have a basic knowledge of copy protection. As we will see in later sections almost all the latest copy protection mechanisms prevent this kind of copying.

3.2 Hacker Groups

There are many Hacker groups out on the internet [CU07] and most are involved with or specialise in cracking computer game and releasing computer games on the internet as what is commonly known as “warez” . They usually compete with one another to be the first to crack and release the new computer game. The more high profile games that are cracked and the quicker they are cracked the more fame that are attributed to that group. Many computer games are released on the internet before the official release date of the computer game and are known as “0 day cracks”

The beginnings of the professional hacker scene can be dated around the end of 1986 [FR05] The first professional groups were formed this time as this happened to be when computer game publishers started to use copy protection techniques to protect their games. Attempts to stop these commercial pirates were in vain as usually a team of hackers were employed who could crack these mechanisms with little effort.

A text file with the extension .NFO is always included with the pirate game by the hacker group. It is basically the pirates’ version of the readme.txt. Originally these text files only contained information about the cracking process of the program. But as time progressed other details were included such as information about the game, quick 'HOW-TO's and release credits. Eventually these text files became more formalized and were included as standard in every release by every group. These can be very useful in finding out which type of protection has been cracked especially if a game has been protected by various types of copy protection. Figure 1 shows an NFO which was found with a pirated copy of tomb raider anniversary. Note that the protected that has been cracked by the group can be seen in this case Securom.

Figure 1 shows part of a NFO that was distributed with a pirated tomb raider anniversary copy.

3.3 Suppliers to the Hacker Groups

Although it is not unknown for external sources to gain unauthorised entry to a developer and steal the code directly [BC03] most suppliers to the hacker groups are insiders. They are a kind of corporate saboteurs for the hacker groups and can range from employees of courier firms, game magazine journalists and employees at mastering facilities and distribution centres. Journalists are seen as the best insiders as they are usually sent the computer game

without any copy protection. An unprotected DVD version of Tomb raider anniversary was released online a week before the official release date [RL07] and possibly came from a journalist sent a DVD preview copy without any copy protection.

The earlier a hacker group gains access to a game the more time they have to break the copy protection and understand the game code (create for example cheating utilities for multiplayer computer game) while other hacker groups are still waiting for its public release

3.4 Distribution

Various peer to peer networks (P2P) are now available to pirate everything digital including computer game. Generally a P2P network refers to any network that does not have fixed clients and servers but a number of peer nodes that function as both clients and servers to the other nodes of the network.

Peter Biddle (PB02) talks about the growth of “darknets” which ranged from ftp servers, newsgroups and email to the now ubiquitous peer to peer networks. These networks are becoming the main methods for distributing pirated computer game and as stated in the section “history of computer games” the peer to peer networks combined with the search engines make finding and downloading pirated games much easier. He found that the tools and documentation for removing copy protection also being distributed through these darknets. He states that for a “Darknets” to grow users need to be connected by high bandwidth networks. So large bandwidths that allow for the distribution of online computer game is also the same channel used by the “darknets”. Pirated computer games are usually distributed as complete ISO images which mean basically making a complete copy of the CD digitally.

3.5 Example of Obtaining a Pirated Computer Game

In the past as described by section 2, piracy was generally an underground activity consisting of private BBS or FTP site. Now the usual way to obtain a computer game (if not buying an

illegal copy in the market or pubs) is to obtain a computer game through a peer to peer network.

The basic five steps are:-

1. Go to Google and search for torrent search sites

2. Once on the torrent search site search for the game title

3. Install a P2P client program

4. Click on the game title link in the search site and download the game

5. play the game directly from the hard drive for PC or burn to a DVD media for consoles

An attempt to find and download Tomb raider Anniversary [RL07] which was released in June 2007 was attempted using the 5 steps above. Appendix 1 contains the screenshots of the steps detailed above which were applied to obtain this computer game.

As we have seen the consumers are not driving the pirated game market as the hackers themselves are not driven for profit. Without the internet pirating would still be happening but the effects to the computer publishers would be far less. Consumers now with the help of the internet find it very easy to find and locate pirated games and are taking advantage. The Internet is not the only reason but also the P2P networks which allow sharing of illegal material with some degree of anonymity and has fostered the easy distribution and sharing of

4. Historical Techniques for copy protection of computer games

Copy protection has been and still is concerned with trying to stop the Sharing of the Installation media or creating and distributing illegal copies of installation media. For years computer game publishers did not even have techniques to prevent casual copying and so

resorted to a number of techniques which just pushed up the cost of the game or were just plain annoying to the consumer and may have put them off purchasing the game.

Initially Copy protection was just concerned with protecting CD s from being copied. The first attempts were undertaken in the 1990s although CD recorders did not exist at this time and developers had to just prevent unauthorized copying of CD contents to hard disks. With the arrival of CD recorders interest in copy protection increased. By the beginning of 2003 there were approx 50 different CD copy protection mechanisms as described by Korba and Kenny [KK04]

4.1 Annoyance

This is probably the easiest implemented form of copy control. The user is annoyed until he goes and buys a licensed copy. In the simplest case this is a screen which pop ups at the application start or while using the application. More sophisticated cases need the interaction of the user, for example users have to push one of three numbered buttons at the start of the game – the correct button is chosen randomly each time by the program itself, thus preventing the user to do this subconsciously after a certain period of usage time.

4.2 Dongles

One of the first hardware techniques to be used was the dongle [TM84]. The dongle is a hardware device usually distributed with the game and is connected to the computer by the serial or parallel port. As the software executes it at certain time intervals it queries the dongle for the output of some secret function. If this fails then the software stops working or cripples itself by returning to an evaluation mode. The dongle mechanism also has several drawbacks as it is generally expensive and will further increase the cost of a game. Distribution is also limited as it is not feasible to include a dongle in a game which is downloaded over the internet. It is also relatively easy to crack this kind of protection by reverse engineering the game code and checking for the calls to the dongle and then bypassing the calls. We will see in later sections this is one of a number of main methods for breaking copy protection. After the game code has been sanitized of Dongle calls a code patch is usually distributed so that

anyone can play without the required dongle. An example of a game using this kind of protection was Robocop3 for the Amiga platform. A dongle had to be fitted to one of the joysticks for the game to run. A few days after its release the dongle protection was cracked

4.3 Instruction Manuals

Another early technique was to use the instruction manual. Every the game had started it would ask for the user to input a word or a sentence from the manual before the game would start. An example would be "what is the 25^{th} letter from the 8^{th} line" It was however trivial to copy an instruction manual using a photocopier or even by writing out the manual by hand! More sophisticated techniques were used such as code wheels. The most imaginative of these was "The secret of Monkey Island" by Lucasarts [LA90] .It had a cardboard wheel with halves of pirate's faces. The game showed a face composed of two different parts and asked when this pirate was hanged on a certain island. The player then had to match the faces on the wheel, and enter the year number that appeared on the islands respective hole.

4.4 Installation Keys

This used to be the most common form of copy protection for PC games. During the installation process the user is asked to enter an installation key in order to verify that the computer game was brought legally. This form of protection was generally easily broken. Installation keys are usually based on some kind of sequence so all the hacker has to do is analyse the algorithm code that determines what sequence of letters and numbers are valid. Once the mechanism is known the hacker can create a "key generator" which will produce the correct sequence of keys to be used with illegal copies.

All the above examples were trivial to circumvent and most relied on the plain laziness of the consumer e.g. not to copy the instruction manual or cardboard wheels. This however was not case and there was always someone with the time and energy to break the system. This is an important point forgotten by the game publishers is the fact that the hacker groups find copy protection a challenge and will spend the time and energy to break a new copy protection

system. The exception to the above is installation keys which although can be bypassed with key generators do allow for a game to be identified. In this case it failed as the game could be identified but the consumer could not be.

5 Contemporary mechanisms to protect physical media

There is no absolute protection against copying of games from physical media. Such a copy protection is extremely difficult to design because if the disc can be read this means there will be some way of copying it. The next section is a review of the copy protection mechanisms being used to protect Computer games. Much of this information was obtained by looking at the protection used on Eidos [EI07] games in the last 2-3 years.

5.1 Protecting the Physical Media from Being Copied Directly

Copy prevention mechanisms for physical media copy protection will look at two aspects, protecting the CD from being copied directly and protecting the files that are on the disk from being copied onto a hard drive.

5.1.1 Basic Overview of a CD

To help understand CD-protection methods a brief overview will now discuss how a CD is organised and how it is read. Physically a CD is a thin plate of plastic with thin reflective aluminium. This layer is then covered by another protective layer. This reflective layer is imprinted with a chain of microscopic “pits” and “lands” arranged into a continuous spiral track. This winds from the CD centre, to its outer edge

Kaspersky [KK04] gives a good overview on “pits” and “lands”. Contrary to common belief these “pits” and “lands” do not correspond to ones and zeros of binary code. The one of binary is represent by change from a pit to a land or land to a pit while the zero is represented by a lack of change for the current interval.
The CD is organised into a frame which is a group of 36 bytes. Frames are joined to make sectors which contain 98 frames. Inside the frame is also a one byte dedicated to what is

known as subcode channels. Each of the eight bits of the byte is designated by a character P, Q, R, S, T, U, V and W. Each of these Bytes from each of the 98 frames is joined up to make a channel through a sector. Usually CD only use two subchannels P and Q. Q is used for determination of the sector on the disk whereas P is used as a termination marker of the current track and a pointer to the next track and basically determines pauses when the CD laser head is moving

The sector is the smallest unit of data that a CD drive can read in what is known as “raw mode”. This means there is no access to actual “raw bytes” ruling out a bit by bit disk copy. This is the main way certain CD copy protection mechanisms can distinguish a copy from an original.

The Compact Disc Digital technology was originally concerned with audio but over time has evolved to become a media for general data storage. The original standard jointly developed by Philips and Sony was called the Red Book standard which was concerned with Audio .Next the yellow book was developed with the standards for the structure of a CD for data storage. The Yellow Book itself is not freely available. However, its content corresponds to the ISO/IEC 10149 and EMCA 130 standards [EC96] Generally speaking most of the following copy protection techniques preventing sector copying of a CD can be divided into the following two types

- Deviations from the standards
- Binding to the physical characteristics of the media surface

Protection mechanisms concerned with non standard can be implemented by not complying with the red\yellow book standards. Most hardware and software will attempt to comply with the standards and so the result is that the protected disk can not be copied using standard methods. It is important to note that deviations from the Yellow book standard could mean that some disks can not be read as due to the impossibility of testing the large number CD devices on the market. Consequently there is a risk that owners of untested models will encounter serous problem. The greater the deviations from the standard the higher the risk of alienating a significant portion of computer game users. New scientist [NS02] reported that the

Philips Corporation strongly opposed any deviations from the standard and insisted that protected discs should not use the “Compact Disc logo”

An alternative to deviation for the standards and the risks that involve is to bind to some physical characteristics on the disk. One method of doing this is to introduce on physical defects on the storage media and damaging the disk surface in one or more locations.

5.1.2 Physical Defects

This can range from using a laser to use pits of varying shapes or carry out manipulations of the density or pattern of the spiral track. When a drive attempts to read sectors located in a damaged area it will generally return an error message such as bad sector. Most CD writers will be able to skip these damaged sectors and copy all the readable information off the disk. However the normal and readable sectors will be located in positions originally occupied by damaged areas. The copy protection system will check for the damaged sectors in the predefined areas and if they can be read then will conclude that the disk is a copy. This method is not without its problems as specialized equipment is needed and therefore the games have to be mastered in a special facility usually with increased costs of manufacture. Also the type of physical defect should be such that the disc does not lose its mechanical strength. A deep radial scratch could mean the CD is torn up by centrifugal forces inside the CD drive. The best method is to create a small pinhole in the reflective layer. Lastly once the bad sectors are known on a disk they can be searched for by reverse engineering the code. Most copy protection systems use to write these “as is” and so the decision making function can easily be found and circumvented.

5.1.3 Key Marks

Instead of physically marking the disk an alternative is to change something on the CD which can not be easily detected or read by a CD recorder. Key marks are such things are stored in sub-code channels. As discussed earlier only 2 of the eight channels are being used by the CD which leaves 6 channels to add in key marks by changing one of the 6 channels. This is only possible on a number of high-end Mastering CD replicators and most normal CD writers will

not copy sub-code channels and hardly any will write to them. To validate an original the copy protection mechanism will check for a mark in one or more of the sub-code channels

5.1.4 Using Existing Uniqueness

An alternative to physical defects is to use uniqueness that already exists. No two CDs are absolutely identical; each CD is characterized by a set of unique parameters that differentiate it from all other CDs. These unique characteristics can be used by protection mechanisms for the identification of original media and weeding out unauthorized copies.

An example of this is the read timing characteristic which is the time it takes for a CD to read a sector or varies from disc to disc. This is then converted by an algorithm into a registration number which the copy protection mechanism keeps securely and a special request code is generated which is reported to the User. The User passes this code to the game publisher \developer from which is passed back the registration code for that CD. The copy protection will then check that the registration code matches that which has been given and if match is found then allow the game to be played. If the disk is copied then the disk characteristic would be different and so the registration code would no longer be valid , However as the protection code can regenerate a special request code and registration number these duplicate copies can be registered legally. Care has to taken that the algorithm generating the registration number has a difficult to find dependence on the request code and the registration number can not be determined from the request code.

The drawback is that if the algorithm is too stringent then users with older drives which distort the timing and may be suddenly recognised as a copy and cease to operate. This may also happen if the CD is slightly damaged in some way.

5.1.5 Weak Sectors

Kaspersky [KK04] claims that this technique when initially introduced was one of the most difficult to overcome. Copying of the protected disk takes place normally and without error but when the copy is checked the check reveals numerous bad sectors. This is the case even if

the file to file protection has been broken and the files are copied from a hard disk to a CD. The reason behind this is weak sectors. These are a certain combination of bytes results in pits dominating lands. This means that the tracker device reading the CD will lose the track it is reading because of insufficient brightness of light falling into the photoreceptor. Most CD writers trying to copy the disk would increase laser power assuming there was something wrong with the disk and usually report that the sector is unreadable and therefore a bad sector. The sector would appear damage on the disk but in fact at a physical level is not. The following figure shows a representation of a weak sector. Note the number of pits and their lengths compared to the number of lands.

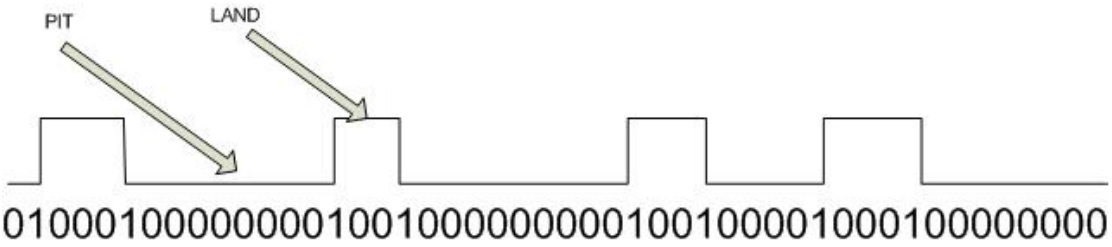


Figure 2 shows a physical representation of 04 B9 04 weak sector sequence

A copy protection mechanism would insert these combinations of bytes into the game executable and possible other associated game files and copy these onto disk using a high end CD production system which will compensate the weak sectors on the original CD. However any attempts to copy the CD with a standard CD writer will result in the weak sectors in the middle of the game executable and hence the copied version will not play.

5.1.6 Check Presence of Original CD

This is the most common protection used. The game would check generally when loaded but it can be at periodic intervals if the Game disk is in the physical media drive. It can use a variety number of methods such as looking for a specific hidden file on the disk or a unique code

specific to that disk. This is rather weak and can easily be overcome by a number of tools which will be described in the attacks section it is still in use but in combination with other types of copy protection.

5.1.7 Blacklisting

Blacklisting involves the detection of hacker tools on the user's computer. For example if copy protection detects a virtual drive then the game will no longer run

5.2 Preventing File to File Copying

Properly designed protection mechanisms usually not only try and prevent copying at the sector level and therefore prevent direct CD coping but they also need to prevent file by file copying to the hard disk.

5.2.1 Non-standard formatting

These methods consist of intentionally introducing specific errors to prevent the normal processing of information. A very simple example of this would be to use invalid file sizes. This technique uses the CD table of contents and creates a fake version. Each CD has a Table of Contents which describes the exact size, location and a filename of every file on the CD. Each protected file on the CD could be artificially increased to 1000 GB and thus in order to copy the protected disk a stack of DVDs or a very large hard drive would be required. The copy protection mechanism would store the actual size of the files and therefore be able to work with them without encountering any problems.

This is a very simple example and such a protection mechanism could be circumvented by copying the CD at a lower level (the sector level). Additional methods can help increase the complexity to the protection mechanism by tweaking the TOC so the disk looks blank or grows beyond a useful cope able size. In the past CD writers which just relied on the TOC

would not be able to copy the CD, although the latest versions of CD coping software can circumvent this by also checking the file sizes directly at the sector level.

Another similar technique is to use dummy files. These mechanisms create ‘Dummy Files’ which are pointing to random parts of the CD, which are already in use by other files. When copying the CD content to hard disk or trying to burn the CD, it seems that it the CD image is much bigger than the Data track size on the Original CD (sometimes the total file size is over 2 GB!). Copying at the sector level will circumvent this type of protection

Obviously it would be an idea to use a custom non- standard data format which could not be accessed unless using a special type of player. However the development of a custom file format requires considerable investment and hackers would still be able to copy it at the sector level and still make copies.

5.2.2 Drivers

Usually access to a CD Drive is through a driver which is in a privileged operating system supervisor mode so that it can gain access to the I/O functions of the OS. Once a game is installed some copy protection systems will replace this driver and once the game is running will intercept calls from the operating system and redirect them through this new pseudo driver before passing them to the actual driver. This gives an advantage in that a CD writer will no longer operate as a writer or certain parts of the CD can be no longer read (e.g. preventing reading of certain subcode channels as discussed earlier)

5.2.3 Encryption

The most widely used technique to prevent file copying by copy protection mechanisms is encryption. Almost all the commercial products out in market at the present time investigated by the author now use encryption. The basic technique is to encrypt the files before writing them to the master disk and then decrypting them on the fly when the game is first executed.

Figure 3 shows a simplified version of the encryption technique. A big challenge with this technique is key management. Usually a secret key is embedded somehow on the physical

media in a way that can not be easily copied. This has been done by using asymmetrical cryptography to encrypt the key. This key is then used by the copy protection system to allow the game to be decrypted into memory.

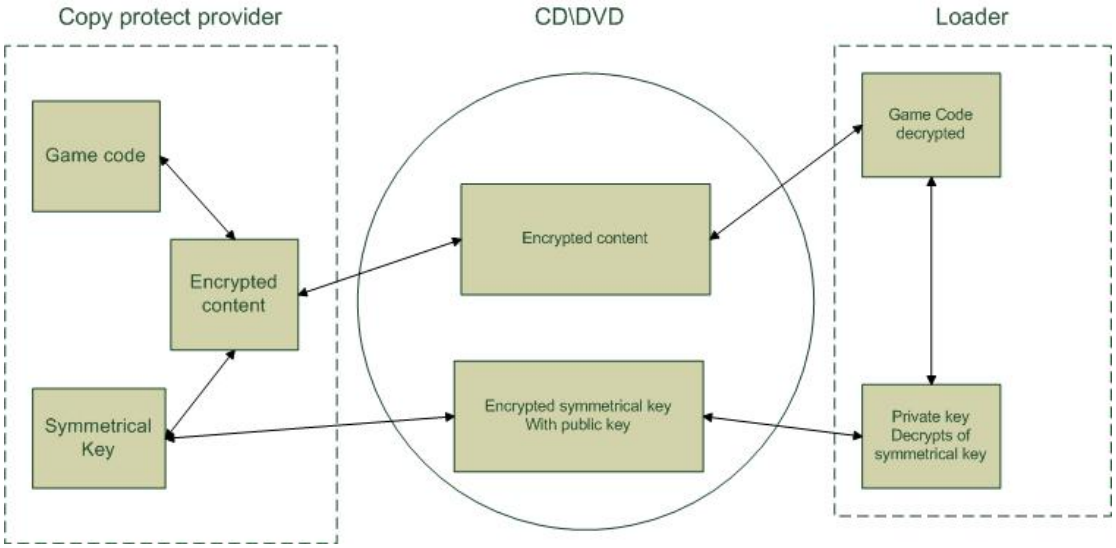


Figure 3 Basic architecture of a software based using the Encryption technique

Most commercial copy protections usually encrypt the main game executable using a symmetric algorithm and key. Asymmetrical cryptography is then used to create a public\private key pair per disk. The symmetric key is then encrypted itself using a public key of the unique public\private key pair. This is then specially burned into the disk during the manufacturing process which prevents it from being copied. A software loader program is then added to the disk which will decrypt the key using the private key and then uses the symmetrical key to decrypt the main executable and load into memory. If the loader can not find the symmetrical key encrypted with the public key then the executable can not be decrypted and the game can not be played.

5.3 Tamperproof Hardware

Lie et al [LI00] describe the use of Tamperproof hardware. This is a method of securing parts of the hardware from being observed by a hacker creating what is known as secure context or secure data storage. A hacker can not gain access to the executing code and therefore identify copy protection code that may need to be bypassed. Console computer games use this technique as the user has to buy a special piece of hardware called a console which usually has several tamperproof security systems.

In the past this has not been feasible for PC computer games but with the development of the trusted platform module [tr07] this may change. The trusted platform module (TPM) is a special chip developed to enable trusted computing features, the relevant ones for copy protection being;

- Memory curtaining – preventing a program including the operation system from reading or writing memory being used by another trusted computing program. This could help prevent memory dumping of a computer game by a hacker

- Remote attestation – Changes to the computer are detected by the hardware producing a certificate stating what software is in use and this certificate can be used to demonstrate that the system has not been altered . This would help with detecting hacker tools on the computer which are being used to circumvent copy protection and verifying that copy protection software has not been altered.

- Sealed storage – Information is protected by encryption with a key derived from the hardware. Information encrypted can only be decrypted on the computer it was encrypted on. The game executable once downloaded is could be encrypted on the machine using sealed storage and thus preventing the game being copied as only that machine it was downloaded on can decrypt it.

5.4 Problems with Physical Media Copy Protection

This section has gone through the latest techniques starting with just preventing the disk from being physically copied with marking, damaging, weak sectors or just plainly not following

the CD standards .Non-standard formatting may seem as a good solution but it does have an issues in that some CD players will not be able to read them and also as the technology evolves CD writers become more efficient and easily circumvent this type of copy prevention. Obviously preventing the disk being copied directly was important but now with the pirate distribution of digital files on the internet it could be argued that it is much more important to protect the files from being ripped off the CD. Therefore techniques of preventing disk copying will probably become more redundant over time.

Encryption seems to be one of the most dominant techniques but there are several problems in that proprietary algorithms have been used rather than public ones which generally have not provided the level of protection that perhaps a public algorithm would have done. Also the encryption is useless once the game has been decrypted in memory. This means that there is no need to attack the encryption algorithm directly. Encryption alone is not the answer and has to be combined with a number of other copy protection techniqes.

Preventing Access to the CD drive by using drivers can be rather risky option as drivers in windows operating systems operate in supervisor mode with potential to access privileged areas in memory containing the operating system. If the driver is badly written it may allow access to the operating system for a malicious hacker. An example of a drivers security problem is when it is installed on a limited-access user account, as might be found on a corporate network. The access control lists of such drivers are set so that any persons with control over the computer, including those without administrative rights, are allowed to change the code that is run by the driver. The malicious user can therefore changes the driver to point at any arbitrarily chosen executable, which is then executed with full system privileges on next reboot. These have been documented in the NIST national vulnerability database for a number of copy protection providers [NV06a], [NV06b]

Tamper proof hardware is seen as the new more efficient method of copy protection as it tries to prevent access to the game code. There could be issues, such as serious risk of data loss in the event that a TPM security chip or hard drive fails. Processes will have to be put in place by the games industry which allows a user to prove an original purchase and somehow obtain a replacement copy.

The next section will look at possible ways to bypass copy protection from both a consumer perspective trying to play a pirated version and from a hacker's perspective in terms of trying to create a pirated copy.

6. Tools to attack physical media copy protections

A large number of tools are available on the market [TT07] which allows a user to play a pirated copy or create one. Most of these tools are concerned with identifying the copy protection, making a direct 1:1 copy or emulating a CD drive and are generally for the consumer to play pirated copies. Reverse engineering tools are used by the hacker rather then a consumer to rip away the copy protection from the game code.

6.1 Identifying the Copy Protection

Physical media copy protections do generally try and hide from the user and make it harder for the hacker or consumer to ascertain which protection is being used .A number of tools have been developed which will identify if a disk is copy protected and which type of copy protection is being used. From this information the consumer can set the tools to bypass that particular protection.

6.2 Direct CD Copier Tools

CD copier tools try and make a direct 1:1 copy of the original CD and bypass non-standard formatting or binding to some characteristic. For example when circumventing physical defects they will recognise the bad sectors and rather than scripting them as would happen with normal CD copying software they will try and simulate them at the logical level. It does this by changing the checksum for a particular sector so that they show up bad to the copy protection software although they are good sectors on the physical copy of the copy.

Weak sectors as discussed was a great copy protection technique however CD copier tools can now cope with these by preparing the sector image in raw mode and search for these unfavourable sequences. By slightly "disfiguring" these weak sectors and recording the

changes in bits. The result is that these weak sectors will be flagged as data errors but will now be able to be read (Pits have been changed into lands) by the CD device. The CD copier tool will correct the data errors and return them to their normal state. Essentially the File is not being totally read from the disk but a very small part (originally weak sector) is being automatically corrected using error information and information recorded about the disfigurement.

6.3 Emulation

Emulation tools are mechanisms that rather than tampering directly with an application, exploit an interface or impersonate presumably-trusted system components.
An example of these set of tools are emulated virtual drives which try and emulates the computer's CD or DVD ROM drives. These tools can read game images created by CD burning software directly from the hard drive. They do not try and make a copy of a game but will try and play a direct 1:1 copy.
Originally they were built to help circumvent the CD-check mechanism but over time they have emulate the copy protections mechanisms themselves for example by correctly identifying weak sectors in the correct places on the virtual disk and thus fooling the copy protection. The real power of these tools is that they allow a direct image to be made of the CD to be saved with the copy protection intact and so no effort is required to strip away the copy protection and create a fixed executable. An example of this is Daemon Tools [DT07] which is a virtual CD/DVD-Rom emulator. Before the virtual drive is started the user has to determine which copy protection is being used by using one of the identification tools above.

6.4 Hide tools

As mentioned earlier in the previous section some copy protections will try and detect if any tools such as virtual drives are present. These tools will then try and hide these tools from the copy protection by intercepting the checks from the game protection software and providing the result which shows that the tool in question is not installed and thus allow the user to continue to use them. A game of cat and mouse then starts as copy protection companies will then try and blacklist the hider tools and the hackers will develop tools to hid the original hiders.

Some copy protections have what is known as an ATIP check. ATIP is a feature of recordable media (such as writable CD) that informs a burner that it is recordable media. The copy protection once detecting the ATIP will stop the game from running in a CD or DVD burner. An ATIP hider tool will help to hide the ATIP from the game copy software again by intercepting the copy protection calls.

6.5 Memory dumpers and Loaders

Hackers can use a number of sophisticated tools to remove the copy protection. Although there a number of techniques they all follow a basic method as explained earlier in this section most game files are now encrypted to prevent file copying. To play a game the code has to be decrypted into memory by the copy protection system so trying to attack the cryptographic algorithm directly is pointless. Hackers will try and use a technique known as a “memory lift”. Here a hacker waits for the authentication checks to take place and the game to begin execution. At this point the game is copied from memory into a file. The normal executable file headers (A header contains general information and addresses needed to access various parts of the file) are then reconstructed resulting in a working unprotected game executable.

6.6 Reverse Engineering

Today’s copy protection code can be a bit more sophisticated and may require reverse engineering to find out how it functions. Reverse engineering is a large area and can encompass a number of processes and toolsets namely disassembly, decompilation and debugging. Decompilation recovers the higher-level program abstractions and semantic structure from binary programs .disassembly reconstructs assembly language instructions from the machine code. Debuggers trace the program logic and data values during program execution. Breakpoints can be set and code and data modified on the fly, making debuggers valuable tools for tampering with applications.

All the above toolsets are used to reverse engineer the copy protection code. An example is copy protection code in the game software checks for an original CD by for example checking for bad sectors on a disk in a predetermined location as explained in the earlier section. The

hacker may try to alter this decision making code to always return “valid” or alternatively try to reverse engineer the decision making code in order to either emulate it, or produce a new valid value for the copied CD.

Together with both memory dumping and reverse engineering hackers will generally try and create automated tools which will automatically circumvent the copy protection. These tools are known as loaders. Loaders will automatically load the game into memory by using the copy protection decrypt functionality and then attempt to patch any authenticity functionality. For example from reverse engineering techniques it is possible for the hacker to note calls to certain functions by name. The loader will automatically search for these functions in machine code and replace them with the hackers fixed code. Once this is done there is usually a possibility of saving the game to disk as what is known as a “fixed executable”. Loaders automate what normally requires knowledge of reverse engineering to the general user population and thus making that particular version of copy protection redundant on a potentially large number of titles.

6.7 Modding

Miles [GM06] details one of the ways hackers attack tamperproof hardware is by “modding” it .There are two different “modding” ways of running pirate code on a game console. One is through soft modding which is modifying the operating system software to allow the user to change data contained on its hard drive in the case of the Xbox. This is relatively hard to do and requires expertise in debugging and reverse engineering another type of modding, known as hard modding this is done by inserting special chips which automatically overwrite certain parts of the bios to disable the checks for original console disks and provide access to the hard drive. Hard Modding requires certain level of expertise in electronics and soldering This is however one of the most popular ways to attack the Xbox or Playstation consoles as consoles can be sent and have the special chips inserted rather than user having to themselves.

6.8 Analysis of the Effectiveness of Tools for Bypassing Protection

Copy protection can be circumvented quite easily using a number of standard tools as described above. Identifying, direct CD copying, emulators and hiding tools are freely available on the internet or can be brought by the consumer. These will allow most copy protections to be circumvented if not immediately then over a short period of a few months after the copy protection is released. Newer copy protections are usually tackled by the hackers using the memory dumpers and reverse engineering tools. Most copy protections routines are programmed to be in the same relative memory space so once cracked the hacker can produce an automated tool or create an add-in to the consumer tools. Blacklisting of tools will try and combat consumers using these tools but these blacklisting tools are looking for certain registry entries or files. Hider tools have circumvented this protection by moving registry entries or files from the default locations.
Another problem which affects all these mechanisms is that although the game can be identified with the use of installation keys, the device or the consumer can not be. Tamperproof hardware does try to identify the device and prevent the hacker from getting to the code but again there is no connection to the user. This is true of game consoles and will be even more so for PCs with the trusted platform module. The trusted module is regarded as a difficult mechanism to circumvent and heralds a new dawn for copy prevention but we just need to look at how consoles with all their tamperproof techniques have been circumvented by modding and no doubt the same could happen with the PC's trusted chip.

Now we have looked at physical media copy protection the next section will look at the new copy protection techniques of games distributed over the internet and examine how effective they are.

7. Copy prevention of online distributed games

With the growth of the internet new business models for computer game distribution have become possible but with new distribution avenues for pirated software have become possible. Distributing computer game on the internet for both publishers and pirates was infeasible since computer games tended to be very large (1-4 gigabytes) and downloading from the internet was not really possible. However with more and more home users with larger bandwidths this has now become a feasible business model.

7.1 Digital Rights Management

DRM (digital rights management) is a system to protect digital assets and control their usage. The core concept in DRM is the use of digital licenses. Instead of actually buying the digital content the consumer buys a license which grants him certain rights of use. A license tends to be a digital data file that specifies certain usage rules. These rules can be as diverse as frequency of access, expiration date, restriction of transfer to other devices and copy permissions. This is unlike mechanisms designed to protect computer games sold on physical media which once cracked can easily be shared on the internet beyond the publisher or developers control. DRM therefore allows for the potential to mange access to a computer game on a persistent basis

DRM originally focused security and encryption which locked content down to just the user that originally brought the computer game , however as the online computer game market has evolved a second generation of DRM has developed as discussed by Renato [RI01] which covers the monitoring , payment process, identification and trading of the computer game asset.

In a simple cryptographic model two trusted parties own a shared key are exchanging material which a third party attacker is trying to intercept and crypto analyse. In a DRM model there is only one trusted party and one untrusted (the end users). This means the end user can not be trusted with a shared secret key or even unencrypted data. As mentioned earlier in threats to computer games many consumers copy games because of price and so in the DRM model it is not possible to separate honest and dishonest users. Once the content has been delivered to the user's device a malicious user has a chance to break the system with unlimited time and resources. This then leads to the same threats as computer game distributed only on physical media. A hacker can break the system and publish his crack onto the internet via peer-to-peer networks and therefore defeat the protection system.

Korba and Kenny [KK02] describe a basic DRM system using client-server architecture.

A DRM system usually has several components

- Content protection mechanism
- A content distribution server
- A license DRM server
- Content viewer

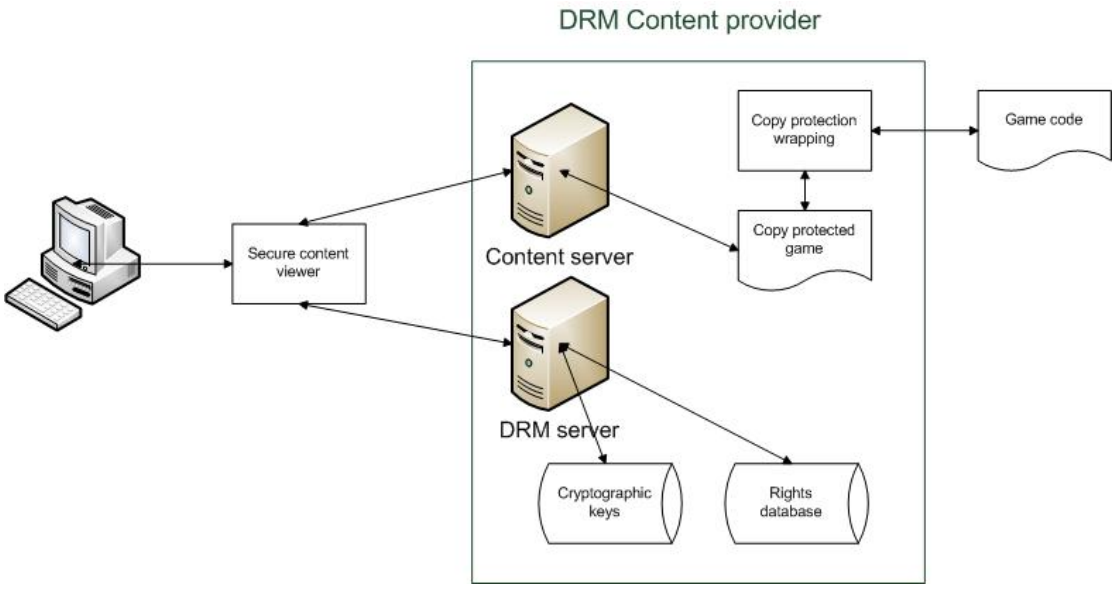


Figure 4 shows the basic DRM process view using the above components [KK02]

The basic process starts with the content provider providing content to be encrypted and protected. This content is packaged along with some license rules or a license key. The license key is saved onto the license server. A typical license rule could be related to the subscription model e.g. 24-hour rental, monthly subscription or available forever but only on one PC. The

protected content is then transferred to the distribution server, physical media or super-distribution. Super distribution is a method which encourages users to pass along digital content, which allows vendors to market their digital content to a vast number of potential customers without any direct involvement and costs. Once the content has been passed along the recipient still needs to obtain a license. It is important to note that super –distribution model only works if the content is properly content protected.

The online customer can either download the content from the distribution server or a streaming server. Streaming is a method that allows the customer to play the game much quicker as the bare minimum required to play the game is downloaded rather than the whole game in its entirety. The content viewer will try to download a license from the license server over the internet. Sometimes a temporary license can be provided, such as a try-before-you buy with a specified time limit. A payment process system kicks in when the temporary license expires and takes the customer payment before downloading a permanent license. An additional benefit of online distribution is that a separate demo does not need to be produced as games can be distributed in full versions with license rules e.g. “try before you buy”

The content viewer provides an important control process as they enforce the protection of the digital\ content based on the license. The content viewer opens and decrypts the digital content. It should be noted that for computer game distribution there are a number of DRM systems each of which uses its own proprietary approach and there is no interoperability

In order for the user to play a game, the content viewer is deployed as client software and has to be installed on their computer. This software handles user authentication and provides secure access to the game. The challenge is to prevent the user from getting unauthorised access to the content by defeating the copy protection system. A number of mechanisms are currently employed and will be described later in this section.

The content viewer verifies that a set of conditions obtained from the license are met when the game first starts and then allows it to run normally if all the checks are deemed to be ok. For example in a try-before-you-buy scenario the content viewer might first check the current date. If this current date is greater than the expiration date the game will display a payment screen.

If this check is passed then the game executable is decrypted and as stated earlier it is now that the game is vulnerable to attack

The most interesting part of DRM for this dissertation is the Content protection mechanism. Liu [QL03] discusses persistent copy protection role in DRM and suggests that the copy protection has to stay with the content. For example a game can be downloaded off the internet securely using standard cryptographic mechanisms such as SSL but the recipient must not be able to make a digital copy once he has received it. Liu also lists a number of copy protection mechanisms involved in protecting against unauthorised interception and modification, unique identification of recipients and effective tamper resistant mechanisms. These will be described in the following sections.

7.2 Asymmetric Code Blending

This technique tries to intertwine the protection code within the game code rather than just wrapping around it and therefore becomes an intrinsic part of the new executable. The code is therefore inside the game executable and thus making it a much more difficult task to remove the protection code from the executable. This means that once the executable is decrypted in memory the protection code is still embedded in the game code.

7.3 Encryption

To prevent easy direct illegal copying of the digital computer game the content is encrypted using a symmetric key algorithm. Obviously the encryption algorithm must be strong enough to prevent easy decryption of the content by brute force or dictionary attack. It also has to be fast so that decryption which occurs on the fly does not impact too much on the user when he starts the game. Whilst researching the DRM providers for this dissertation noted that a lot of DRM providers keep their encryption process and algorithm details confidential. This is “security through obscurity “and does not allow for the verification of the cryptographic algorithms employed in the same way as public ones. Stamp [MS02] found that compared with standard implementations of cryptographic algorithms, non standard implementations of such algorithms are not trustworthy and probably not as efficient. Activemark [KK04] state

that they are using advanced encryption standard with 128 bit key although just like encryption with physical media most others are keeping the algorithm a secret or are using proprietary mechanisms.

Asymmetrical encryption is used to encrypt the digital license which contains the symmetrical decryption key. The license is encrypted with the content receivers' public key and the private key is stored securely in the content viewer. This means only the content viewer holding the correct key can decrypt the symmetric key and play the vide game. This is similar to how the Encryption and Loader techniques works as described earlier in section 5.2.3

To prevent unauthorised modification to the license one way hash functions are combined with digital signatures to ensure integrity of the license. The DRM provider will use its private key to sign the hash function of the encrypted content rights. The content viewer will decrypt the signature using the public key of the DRM provider and then comparing the hash value with a re-computed hash value.

7.4 Binding to a Device

Most DRM providers rely on a unique identification of a user's device. Each license is bound to a device such as a PC. This means that the license can not be transferred or used by another device. The following is an example of how this works for vide game downloads onto a computer.

When a content viewer is first downloaded a unique DLL (dynamic link library which is a collection of small programs that can be called by a larger program) is created along with hardware ID. This hardware Id is created from examining the computers hardware and combining data such as Disk hardware ID, CPU speed, and mother board serial number into an algorithm. The DLL is bound to the computer using this hardware ID and also a public\private key pair is generated. The private key is stored securely in the DLL file and only accessible if the hardware ID algorithm is proved correct. The corresponding public key is used as the players' identifier when requesting a license and the DRM provider will encrypt the license using this key. If the encrypted computer game is copied to another computer along with the download license a content viewer either has to be installed or the original content

viewer has to be copied and moved. However a new DLL is automatically created as the old DLL file will no longer be accessible as the hardware ID will be different. This also means that the license copied across can not be read as the private key in the original DLL can no longer be accessed. Most games distributed today are using the super-distribution model as discussed earlier in this section and will usually revert to a demo mode or try-before you buy. A new license can be requested using the new public\private key pair before the full game can be unlocked.

Binding to a device can reduce the damage caused by cracking because if the DRM is compromised only that device or user is affected, however it does introduce a problem with portability. Every time he reformats his computer or upgrades to a new computer he has to acquire new licenses. This has been somewhat mitigated by some DRM providers by allowing the user to backup their licenses and restore to another computer usually only for a number of fixed times.

7.5 Digital Watermarking

Digital watermarking is an imperceptible message which is inserted into the digital content. It is usually concerned with binding information such as content owner to the digital content.

Watermarking can be used for access control [JD01]. Ditterman shows that the watermarks can be used to verify the allowable number of playbacks and secondary copies. When the content viewer accesses the digital content it counts the number of watermarks embedded in the content, checks the license usage restrictions and then updates as required the watermarks. The big advantage is that it binds usage rights to the actual digital content no matter where that content travels. However current watermarking is not perfect and is really limited to music and digital photographs. Generally if an attacker knows the watermarking content then he can mangle the watermark beyond recognition [MS02] and most known watermarking techniques are not robust enough to prevent a hacker using reverse engineering to identify and remove the mark .

A solution put forward by miles [GM06] which claims to be robust is to use watermarking which is generated during the execution of the program. The fingerprint is generated as the

program executes through the fingerprint branch function. The fingerprint is created dynamically and only exists during the execution of the program therefore can not just be found by reverse engineering. A problem with this solution is that games have to efficient especially when displaying 3D graphics and it could be that that such a branching from the normal execution path could affect game play.

Most game publishers use basic watermarking to trace where a cracked game originated from. This is particularly useful when game copies are being distributed to journalists and other public relations personnel. Watermarks used on their own for any kind of commercial computer game distribution is not really possible for reasons explained above.

7.6 Code Obfuscation

Chang [HC01] describes code obfuscation as source code that is (usually intentionally) very hard to read and understand. Basically it is the idea of taking a program as input and producing another one as output. The output program is unintelligible and difficult to read. Chang lists three types of obfuscation

- Layout obfuscations alter the information that is unnecessary to the execution of the application such as identifier names and source code formatting (e.g. removing of comments)

- Data obfuscations which alter the data structures used by the program (e.g. a two dimensional array could be folded into a one dimensional one)

- Control flow obfuscations which disguise the true control flow of the application e.g. (inserting dead code or merging multiple functions into one)

Some authors [BB01] have found on their own obfuscation does not provide the level of security that encryption provides. It may also bloat up the code and make it less efficient. A less efficient game code can affect the game playability and is therefore unacceptable. It therefore tends to be limited to obfuscating the DRM functional code as an additional measure to supplement the encryption.

7.7 Taking Control of the Operating System

Although this is a possibility for a DRM system. As described in the previous section concerning taking control of the operating system can lead to hackers using the DRM code to gain unauthorised access to a user's machine and is generally avoided.

7.8 Triggers

This technique was described earlier on in the software based techniques section but the DRM version has greater integration with the game code and so requires a greater level of communication between the games developer and the DRM provider. Once a game has been copied it will seem to work perfectly but after a specified amount of time or a particular point is reached in the game then the game will slowly start to fall apart. Cars will no longer steer, footballs fly away into space, guns will no longer fire and enemies become invincible. Those that had been enjoying the game and want to continue are more likely to buy a legal copy then if the game just stopped immediately.

Every so often during points in the game, the game code will check for the existence of the DRM code. This is done by burying certain system game variables within the DRM code (e.g. number of lives, health of enemies). If this code is stripped away to allow for a pirated copy to be made then these variables are no longer available and the game uses "bad" default variables. The interesting trick is to then defer the error until a later point in the game such as when the user reaches level 3. Deferring the error acts like a silent alarm which disguises the point of failure making it more difficult for hackers to identify whether they had created a successful crack or not.

Although a hacker once realising for the presence of triggers can reverse engineer the game code and replace the variables, any number of these Triggers can be set up in any part of the game code and thus makes it a far greater challenge than just stripping away the DRM code itself.

One disadvantage of trigger API's is that many more customer support calls may arise from the game slowly degrading and there needs to be a way for customer service to tell whether a game is a real version or a copy. One technique is to subtly change the way the game looks. For example for a football game the team strip could turn to purple. A customer support team member would first ask the customer to describe the strip colour before going any further.

7.9 Mutation and Content Individualisation

Just like the virus writers try to add functionality that make their viruses and worms appear completely different so that anti-virus software can no longer detect them , DRM providers now also have the technique of making a number of different executables which look completely different at the assembly language level. When a customer makes a download request he will be directed to any of a set number of different executables of which he has no control on which one. When used with Code Obfuscation this can greatly increase the difficulty in producing a generic crack as a successful crack is useful only for the instance of the code cracked

7.10 Online Accounts

An online account encompasses the management of access to and further usage of a computer game. Unlike music or videos computer games have the potential to be upgraded with new levels, maps and additional weapons. This means that there exists an incentive for a user to continue with an online relationship with the games developer or publisher.

Online accounts force the purchaser of a computer game to validate it via an online platform. If illegal use is detected the account may be disabled instantly. Game access activation can be once during the games install or repeatedly over a given period or even every time the game is played. This gives the DRM provider an ongoing control system to identify illegal licenses. Although a user may have successfully registered an unlicensed copy of a game when he first managed to install it, at any time the illegal license may be detected and the account disabled. Cracking a games DRM code is not just sufficient any more. This is in contrast with Retail games played offline on PC's which once cracked allow many users to play pirated software. Additionally when a system is logged into an online account the system can be checked for

undesirable tools. Although as described earlier hiders tools exist, an online platform quicker updates to the search mechanism provides a far quicker response in the cat and mouse game between developers and hackers.

The best example of this is Steam [ST07] which was the first online usage control used for a retail game by valve [VA07] the makers of the very popular Half-life 2. This is the most popular online distribution system with valve claims has 13 million active accounts. Using Steam, players can either download games directly from Valve or register physical media brought in a shop. In either case that copy of the purchased game is directly linked to a personal online account on the Steam platform. This game copy cannot be transferred without either passing on Steam account details or in the case of shop bought games, getting a new CD key.Valve uses Steam to verify legitimate access keys and keep control of further access to its games. It also administers customer billing, provide updates and allow backup of games onto DVDs.
When a game is downloaded with steam not only is online activation required which checks that the license key has not been used before but also a personalized online account with steam. If steam detects any identical licenses it will instantly cancel all those accounts that have used these licenses. This does mean that the user that originally obtained the license illegally is also cancelled and needs to go through a complicated process to revalidate. This does however prevent the consumer from allowing his license key to be used for causal copying. Although steam checks when the game is played in single person mode its real strength comes with the multiplayer option. A user must have an active online account for the game to have access to the multiplayer servers.

Another new development with Steam is that the game is updated automatically every time the user logs in. The user has no control over this process and it happens automatically. The advantage of this is that if any cracks do appear the game can be automatically updated to mitigate any copy protection risk. Games on steam can be distributed on physical\ media but the CD-key has to be registered online with valve and an account set up

Myles [GM06b] gives the example of how Microsoft uses online accounts to help prevent “modding” which was described in section 6.7. Xbox live is an online platform for xbox360 consoles and just like steam the user has to have an online account to play multiplayer games .

When an Xbox user logs on, their system is checked for the presence of mod chips. If mod chips are detected then the Xbox's serial number is recorded and the device is permanently banned from the network. The mod producers however now provide a switch with the chip so it can be turned off when on Xbox live. This does mean they can only play copied games when not connected online but for multiplayer they must have a legal copy. This again shows the use of multiplayer games to help prevent piracy.

7.11 Comparison of Online Distributed Copy Protections

With the advent of Digital distribution on the internet we have seen a number of improvements in copy protection as compared with physical media protection.

We can see that unlike DRM for video or music, with computer games it is possible to wrap copy protection inside the computer game code. Asymmetric code blending and triggers are imbedded into the code itself and can be implemented any number of times within the same game code. This now makes standard tools described in section 6 much harder to use as the code protection code is now not standard and can vary from game to game or even between game version updates .

The copy protection is now also hiding itself from attack. Code obfuscation, code blending and mutation are designed to make the code difficult to reverse engineer even if the game is dumped out of memory. It also prevents the functionality algorithms from being always in the same place within the code base and changes the relative memory locations each time the game is played. As memory dumping becomes harder the encryption algorithm will be probably become a target but having learned previously from CD copy protection the encryption algorithms are now tending to be public rather than proprietary.

All the above techniques will only slow down the hacker groups but as we have already mentioned hacker groups do consist of people with a lot of time and determination. Online accounts do however mean for the first time that the game and the consumer can be identified. There is now a link between the consumer and the game copy that they are using. This is a big step from physical media in which only the game could be identified. Registration online

means that there is a permanent link between the account and the installation key, and that key can no longer be used with other accounts. In the future it may replace most other types of copyright protection.

Problems however do exist with online accounts as they really work best with multiplayer games .The stick to keep the consumer legal is the threat of being banned from a multiplayer platform. Single player games will probably still be cracked and used by consumers as shown by Steams ‘half-life 2’ game which was cracked but only works in single player mode. The other big disadvantage is that once an installation key is stolen then the legitimate users copy as well as the pirate one is banned. There needs to be a process to allow the legitimate copy back on and stop the pirate copy from returning.

Computer games are being released on both physical media and online. This results in a number of different copy protections being used. These copy protections may for example differ in the number of files they encrypt or how they are linked to the game code via for example triggers. Copying files from one copy protection to circumvent another will become prevalent until the games industry decides on one type of copy protection method. In my view in the next few years physical media and online protection providers will become interchangeable with the game being still sold on physical media without any physical media copy protection but with the requirement to register the game with an online account.

8 Attacks on online distributed Copy protection

With the whole array of new techniques attacking online copy protection is much harder than with just physical media however as with all types of security systems vulnerabilities do exist and the following section lists a number of them.

8.1 Demos and Betas

Game publishers and developers are often sending games via the public relations department to game reviewers. Due to the pressure of release dates these games are not protected and are sometimes full versions of the game as in the tomb raider anniversary case[RL07] .Some

publishers now often only send demos which consist of a few game levels only . These are however still good sources of information for the hacker who use the unprotected demo version to compare against a protected version to help identify valid information that is not visible in the protected version. This technique has become particularly important in circumventing triggers as the hacker can ascertain the correct variable that should be supplied to make sure the game plays correctly.

8.2 Reverse Engineering

Although reverse engineering is made harder by the techniques describe above there have been attempts to try and break them. The best way to illustrate how these protections can be broken is by looking at one example. There are large numbers of DRM Solutions in the market but one of the most used in the computer game industry is Activemark developed by the Macrovision Corporation. The latest version at time of writing is version 6. It is being used extensively in the games industry and therefore has attracted attention from a number of hacker groups.

Activemark uses most of the techniques described in the previous section. This software protection system improves upon previous versions by employing more strategic code obfuscation and literal string encryption. This new version now allocates memory to include a random value that is used in conjunction with the CPUID instruction (processor identification instruction) to enforce running the executable on a single machine to thwart the distribution of any pirated / copied applications. ActiveMark also utilizes a method called active memory scanning which uses CRC to check for any changes in the code. It also unlike other copy protections will not decrypt all the code for an application. There are now several layers the 1st layer decrypts the code for the new 2nd layer, which in turn decrypts the code for the 3rd layer and the original code .This original code has a number of triggers to check that the 3rd layer is still present. Of course all these layers mean that a game will take longer to initialise and start.

A number of ways exist to attack this protection. A number of tools and tutorials to dump ActiveMark can be found on the P2P networks. The basic method is to dump bypass the first two levels and dump the level 3 ActiveMark code with the code. Templates developed by the

hacker groups contains code that bypasses calls for expiration dates or timer and the browser nag screen and return the correct values that the Activemark is expecting from these calls . Due to code obfuscation the templates can not be applied automatically and the function addresses have to be manually searched in the code and then the template applied at various points of the ActiveMark code which will basically turn off the calls to the ActiveMark copy protection at level 3 from the game code. If a game code has triggers then the above method will not work as these are individual to a game or to a particular executable version.

8.3 Pirating Multiplayer Platforms

Online accounts are seen as a big leap in preventing piracy. Steam was the first to use this concept fairly successfully. However, one vulnerability is that Steam provides server software so that users can run their own servers and host multiplayer games. These online servers will contact Steam and verify the online accounts. Hackers rather than attacking Steam itself have started to attack the server software and prevent it from calling Steam and thus allowing original and copied games to play on the servers.

Another example of this is from Blizzard [BL07] which has an online platform called battlenet which like steam validated a user's license before allowing access. A group of pirates reverse engineered the protocol language which communicates between the game and the online platform. This meant they could set-up their own online environment which allowed users with pirated copies to play as the License checking routines and account disable functions were turned off.

8.4 Analysis of the Effectiveness of Online Protection

We can see from the Activemark example that copy protection techniques although not being totally secure are harder to bypass and require a lot more time and effort from the hacker particularly if techniques such as triggers are being used.

We can see from this section that the focus is moving away from attacking the copy protection directly and attacking the infrastructure that support the copy protection such as replicating the

multiplayer platforms. Although this is a comparatively large undertaking compared with copying the game it would be of no surprise to have more thypes of multiplayer game server software reverse engineered to allow pirated copies to play. This may allow hacker groups to be located just as happened in the past with hosting of BBS described in the section 2. However now with the global reach of the internet the infrastructure could be hosted in countries with little or no legal copyright law as is the case with email spam servers. If the server software becomes the target of attack then it would be interesting to see if copy protection then also starts to include this as well as the game code. However as we have discussed earlier in the introduction most computer games sales occur in the first 6-8 weeks so the protection really only has to provide protection for 3-4 months to be at its most effective for preventing piracy's impact on sales. It could be argued as long as the protection stops automated hacks and cracks being implemented then this is sufficient. All the research and design that has gone to produce these techniques cost money and over time copy protection has got more expensive. Rather than spending money on expensive DRM systems it may just be enough to use one technique such as online accounts which can be built into the multiplayer and online distribution platforms.

The next section will put this to the test by analysing how long physical media protections and online protections are taking to be cracked.

9 Examination of the effectiveness of physical media copy protections compared with online copy protection

It has been assumed with all the new techniques described in the last section that online protection is more effective than physical media protection. Various DRM providers such as Steam are claiming this is in fact true. To test this, a number of Eidos games released online and on physical media were tested over a period of months. As mentioned earlier in section 3 and demonstrated in appendix 1, almost all pirated software can be obtained on the peer-to-peer networks or on internet sites with cracks. One method to look at the effectiveness of copy protection is to examine how long from its official release date does it take for either a crack to appear or a complete ISO image of the pirated game. A crack will allow any one to make a complete ISO image of the pirated game. As we have seen all hacker groups will race

to be the first to release a pirated version of a game and therefore very soon after the game is cracked it can be assumed the game will be released on the internet.

Taking this last assumption we can therefore track the internet sites and look for cracks and ISO's for particular game titles.

9.1 Methods

Software was examined that would check a number of web sites and crack internet sites on a daily basis. A program called Check&Get will monitor web pages for updates and notifies when changes were made to that page. It also save a snapshot of the page for offline viewing, detect dead-links, duplicated and mirrored web pages and allows you to search and sort your bookmarks by URL, description and keywords.

A virtual server using software from Vmware was set up with Windows XP and Check&Get. It was decided to use a virtual server due to the amount of viruses and Trojans masquerading as game cracks. This would give the ability to roll back if the computer got affected

As an employee of Eidos it is possible for me to know the copy protection being used for a number of releases during the period of analysis and the techniques being used such as for example triggers. In addition it is possible to know the release dates a long time before they are officially released.

A number of well known crack sites and peer -to-peer search engines were chosen for monitoring purposes. Table 1 gives the list of sites used and their type.

Pirate site	Type	address
ISOhunter	Search engine	www.ISOhunter.com
piratebay	Search engine	www.the**piratebay**.org
Megagames	Crack site	www.megagames.com/gcracks.html
Demonoid	Search engine	www.**demonoid**.com/

Gamedemon	Search engine	www.**gamedemon**.org.
Nforce	Crack site	www.**nforce**.nl
Gamecopyworld	Crack site	**www.gamecopyworld**.com/

Table 1 – Monitoring sites list

These sites were all well known P2P search engines and crack sites. P2P search sites will tend to have the full game as a CD image ISO, which can be burned to disk or played directly form the hard drive using a virtual drive. The Crack sites only contain programs which will disable or bypass the copy protection on an original CD.

A number of Eidos games were selected for monitoring with one of the following criteria

- Game is released on physical media only
- Game is released online only
- Game is released on physical media and online

As a hacking group can obtain the crack a few weeks before the official release date it is not unknown for a crack to appear before the official release date was decided to monitor one month before the official release date. If no crack or ISO was found after a month then the monitoring was stopped.

The Check&Get software was setup to email any changes to particular web site pages. For example for game copy world the Tomb raider anniversary crack was monitored by checking updates on the “T” index page and search engines were searched for the selected titles. Any changes notified were examined for the selected Eidos game titles and any pirated information concerning the monitored games, were noted.

The next stage of the process was to check the cracks or the pirated ISO files and make sure they worked. In the case of a crack this was tested against an original CD. In the case of an ISO image this was tested to make sure game play operated. If techniques such as triggers were used then the game was tested up to the first trigger point and changes to the game were noted. The NFO file which hackers always include with the game was also checked for the

protection cracked. This is very useful when a game is released both on physical media and online.

Due to online distribution being at the time of writing not as significant for consoles as PC it was decided to only look at PC formats.

9.2 Results

Title	Format	Released	Protection	ISOhunter	Gamedemon	piratebay	Nforce	Megagames	Gamecopyworld	Demonoid
CM 07 (MID SEASON UPDATE)	**PC download**	**15-Mar-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
Who WANTS TO BE A MILLIONAIRE GERMAN AND ITALIAN LANGUAGES	**PC**	**30-Mar-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
300 - MARCH TO GLORY	**PC**	**30-Mar-07**	**securom 7**	**27/03/2007**	**27/03/2007**	**27/03/2007**	**27/03/2007**	**29/03/2007**	**27/03/2007**	**NF**
CHAINZ 2: RELINKED	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
LUXOR: AMUN RISING	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
SUPER COLLAPSE! 3	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
JEWEL QUEST	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
SEVEN WONDERS OF THE ANCIENT WORLD	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**

Title	Format	Released	Protection	ISOhunter	Gamedemon	piratebay	Nforce	Megagames	Gamecopyworld	Demonoid
CUBIS 2	**PC download**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
ZENDOKU	**PC Download**	**20-Apr-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
STACKED	**PC**	**20-Apr-07**	**securom 7**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
ANCIENT WARS: SPARTA	**PC**	**20-Apr-07**	**Targus 4**	**01/04/2019**	**01/04/2019**	**01/04/2007 - fake**	**01/04/2019**	**01/04/2024**	**01/04/2019**	**01/04/2019**
ANCIENT WARS: SPARTA	**PC download**	**02-May-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
MERRY GO ROUND DREAMS	**PC download**	**02-May-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
DINER DASH	**PC**	**10-May-07**	**securom 7**	**08/05/2007**	**08/05/2007**	**08/05/2007**	**NF**	**NF**	**08/05/2007**	**NF**
PONY FRIENDS	**PC**	**18-May-07**	**securom 7**	**10/05/2007**	**10/05/2007**	**10/05/2007**	**12/05/2007**	**12/05/2007**	**10/05/2007**	**NF**
BIONICLE HEROES	**PC**	**18-May-07**	**securom 7**	**16/05/2007**	**16/05/2007**	**16/05/2007**	**17/05/2007**	**17/05/2007**	**17/05/2007**	**NF**
PANDEMONIUM	**PC download**	**28-May-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**

Title	Format	Released	Protection	ISOhunter	Gamedemon	piratebay	Nforce	Megagames	Gamecopyworld	Demonoid
TOMB RAIDER ANNIVERSARY EDITION	**PC download**	**01-Jun-07**	**Activemark 6**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**	**NF**
TOMB RAIDER ANNIVERSARY EDITION	**PC**	**01-Jun-07**	**securom 7**	**25/05/2007**	**25/05/2007**	**19/05/2007 - FAKE**	**25/05/2007**	**25/05/2007**	**25/05/2007**	**25/05/2007**
25 TO LIFE	**PC**	**01-Jun-07**	**securom 7**	**29/05/2007**	**29/05/2007**	**29/05/2007**	**29/05/2007**	**01/06/2007**	**30/05/2007**	**02/06/2007**

NF= Not found

Fake = Crack did not function and was a trojan

Table 2 Results of the Monitoring for pirated software for physical media and online media

Table 2 shows the results obtained. The results show that physical media protections are being circumvented far easily than online. 7 out of 9 PC games released on physical media were cracked whereas no online distributed games had any cracks. Games which were released online and on physical media were pirated by circumventing the physical media protection rather than the online version. In general many of the results show that the cracked game is usually available before the release date.

The results suggest that cracks available a week before the release dates were fake and were in fact malware. A big computer game title such as tomb raider will generate excitement within the game user's community and Malware writers are using this to entice people to download their cracks before the hacker groups have managed to release the real crack.

9.3 Discussion of the results

As shown by the results most of the games released on physical media were cracked before the official release date. This shows that probably the suppliers to the hacker groups are operating within the supply chain as suggested in section 3 (mastering, distribution and storage). The tomb raider anniversary crack was actually an unprotected DVD. This DVD was identified by the Eidos mastering department as a German version sent by public relations to one of a number of German journalists.

Tomb raider and Sparta were both released online and on physical media. Sparta was released a week on physical media than online and therefore it was with no surprise that the physical media one was cracked first. Tomb raider was released simultaneously and the physical media was cracker rather then the online. This does suggest that physical media is easier to crack than online. In support of this is the fact that no online games cracks were found. However it should be noted apart from Sparta or tomb raider all other online games were targeted at the casual games market which generally has a consumer base of females from the mid-30 who generally do not participate in game piracy.

Another interesting result is that ‘Who Wants To Be a Millionaire?’ which was released on PC using the same copy protection as the rest. However it was only for the German and Italian markets. It could be that the hacker groups only crack the largest titles such as English or it could be that Who wants to be a millionaire English which had already been cracked works with international versions and therefore there is no need for a specific crack to be produced. Further work could investigate if language of a game affects the chances of it being hacked and the reasons behind this.

Another reason could possibly be although the online games in the sample have achieved significant sales they are not the Top titles. This means that the hacker groups are not focused on cracking online protections at this time as all major titles are released on physical media if not before the online release then shortly after. Once major titles are released online only then the hacker groups will no doubt put in more resources in attacking these online protections

Once online consoles games sales have increased further work could look at the copy protection of consoles both online and physical media and compare these to PC formats.

10 Conclusions

Physical media protections have to protect both the physical media and prevent file to file copying They have tended to use rather draconian methods to prevent copy protection some even going to the extent of damaging the CD and introducing drivers with system privileges has lead to many problems with game play . Online distribution does not have the issue of protecting the installation media only the digital asset itself. Physical media could be described as a closed system with computer games being played by a user on a single machine. Once a crack was produced it could be used on any of the original copies in circulation. Online distribution allows

for a rapid response to cracks and can change the game executable being delivered online to another version very quickly and thus forcing the hacker to start the job again of cracking the new version.

All copy prevention techniques cost money which is added into the game price. Some of them have caused resentment among computer game users especially when the computer is left open to hacking and system instability. This has lead to several boycotts of game publishers by disgruntled computer game users. It is important from a public relations viewpoint that the copy protection is as invisible to the consumer as possible.

Hardware technology such as the trusted computer chip, along with the evolution of DRM to protect online assets could make cracking extremely difficult, but as we have seen there are no absolute mechanisms for protection against copying of computer games. Nothing prevents a hacker group from trying to modify the firmware or introducing certain modifications and thus blocking the protection mechanism. As we have seen in this dissertation there is always race between the copy protection providers and the hacker groups and requires continually copy protection versions to be produced.

Avenues of distribution by for example public relations should be controlled. As shown by the Tomb Raider Anniversary example journalists may also be sources for the hacker groups. It could be suggested that PR should distribute the game online. Online distribution is harder to crack using a streaming method, all the game does not necessarily need to be provided for the purpose of a review. (e.g. only the first 5 levels of a game are provided) and a try-before-you-buy time limit could be used to prevent the game being played after the official release date.

There will always be hacker groups but one of the major sources for technical information on hacking in this dissertation came from the hacking community itself. Emailing a hacker and asking how he did it is enough, and he'll sometimes reply with the actual source code of his hack. If one hacker came up with a foolproof way to get past the copy protection in games but kept that information to himself then Piracy

would not be seen as a problem. Pride is a major factor in the mind of the hacker, and he will post his hack on the forums or release it on peer-to-peer networks usually along with how he did it. Copy protection providers and games developers therefore need to watch very closely the hacking community.

Historically most types of copy protection just stopped the casual copier and only a limited number of consumers were obtaining the cracks, however with the evolution of the internet and broadband access a far larger number of consumers are reaping the benefit of the hacker groups. More sophisticated copy protection is needed and this may have arrived in the form of online accounts giving the ability to lockdown a game to an individual consumer.

11 Future of copy Protection

In the future with the broader acceptance and increased bandwidths to users homes online distribution will most probably take over from physical media distribution in terms of sales. The use of DRM is likely to increase with more types of trusted hardware implementations appearing. The trusted chip has been seen by the games industry as the way to stop piracy but hacker groups have the time and determination to bypass anything that can be reverse engineered as shown by the game console modding.

Customer resistance may be an issue in any future protection implementations. There was some initial resistance to online accounts but it has generally been accepted by the gaming community. Compare this to the bad press that the music industry has got from using DRM on music files.

It may be that instead of attacking the pirates, the distribution networks will become the focus. From a legal perspective and this could mean outlawing of peer to peer software and internet search facilities. This however would be as hard as trying to

outlaw spam distribution servers as some countries will not sign up to international laws or treaties.

Games developers will almost always include multiplayer options in their games which will enforce a connection between the consumer and the developer. For the first time in the history of copy prevention the developer now has many more options then ever before to control who plays on which device. As Microsoft Xbox and Steam have shown piracy will become much harder to bypass and involve much more effort from the hackers such as producing their own rival online platforms

Long term the computer will evolve into the media centre of the living room. Obtaining games may be like watching an on-demand movie with the same type of rent business model. This means games will no longer be for sale on physical media and as online technology develops it may be that only the part of the game being played will be available on the device at anyone time.

Will there ever be a perfect copy prevention solution for games? Online accounts look the most promising but as we have shown in this dissertation there will always be a race between the games developers and the hacker groups and it is usually only a question of time and motivation before the protection is broken.

Bibliography

[BA06] Business Software Alliance - FOURTH ANNUAL BSA AND IDC GLOBAL SOFTWARE PIRACY STUDY -2006 http://www.bsa.org/globalstudy/upload/2007-Global-Piracy-Study-EN.pdf (visited May 2007)

[BC03] BBC News – Half-life 2 code leaked online – 2003 http://news.bbc.co.uk/1/hi/technology/3162074.stm (visited 12 June 07)

[[BC04] BBC news – Chinas online sales double -2004 http://news.bbc.co.uk/1/hi/business/3402011.stm (visited 17 July 07)

[BC05] BBC News – xbox360 copy protection cracks – 2005 http://news.bbc.co.uk/1/hi/technology/4530702.stm (visited - 17 June 2007)

[BB01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan and Ke Yang - On the (Im)possibility of Obfuscating Programs - *Advances in Cryptology - CRYPTO `01*, vol. 2139 of Lecture Notes in Computer Science- 2001. Springer-Verlag.

[BG04] Ben Garrett – Online software piracy of the last millennium – 2004 http://www.defacto2.net/web.pages/online software piracy of the last millennium.pdf (visited 5 June 2007)

[BL07] Emulation of battlenet FAQ - http://www.battle.net/support/emulationfaq.shtml (visited 2 June 2007)

[BS92] Bruce sterling – The hacker crackdown, Law and order on the electronic frontier 1992 ISBN 0-553-56370-X 1992

[CU07] Hacker Group – Curse-x, http://forum.curse-x.com/older-applications/15426-game-hacker-group-app.html (visited 2 June 2007)

[DT07] Daemon tools – http://www.**daemon-tools**.cc/ (visited 5 august 2007)

[JD01] Jana Dittermann, P Wohlmacher, R Ackermann – Conditional and user specific access to services and resources using annotation watermarks – communications and multimedia security issues of the new century – 2001- Kluwer academic publishers

[EC96] ECMA International - Standard ECMA-130 Data Interchange on Read-only 120 mm Optical Data Disks CD-ROM - 1996
http://www.ecma-international.org/publications/standards/Ecma-130.htm (visited 12 August 2006)

[EI07] Eidos – www.eidos.com (visited 6 July 2007)

[ES06]Entertainment software association – Top 10 industry facts
http://www.theesa.com/facts/top_10_facts.php (visited 1 June 2007)

[FR05] Tamar Polgar - Freax: Volume 1 2005 - ISBN 3981049403

[GC06] Galactic civilisations forum – Galactic Civilizations II, copy Protection and piracy - http://forums.galciv2.com/index.aspx?forumid=161&aid=106741&c=1 – (visited June 2006)

[GM06] Ginger Miles, Stefan Nusser –content protection of games- IBM systems journal- Vol 45 no 1 -2006

[Gm06b] Ginger miles -Preventing Piracy within the games industry - The international digital media & arts association journal vol2 no1 - ISSN: 1554-0405- 2005

[HC01] H Chang, M.G Atallah – protecting software code by guards. ACM workshop on security and privacy in digital rights management –CCS -8 DRM 2001 ISBN 3-540-43677-4 Springer

[II07] International Intellectual Property Alliance - 2007 Special 301 Report http://www.iipa.com/2007_SPEC301_TOC.htm (visited 12 June 07)

[JB05] Dr Jo Bryce, Dr Jason Rutter - FAKE nation –A Study into an Everyday Crime. Organised Crime Task Force, Northern Ireland Office (Belfast). - 2005 http://www.nio.gov.uk/fake_nation_-_a_study_into_an_everyday_crime.pdf or http://www.cric.ac.uk/cric/staff/Jason_Rutter/papers/FakeNation.pdf

[JL07] John Leyden -The Register – Blu-ray DRM defeated http://www.theregister.co.uk/2007/01/23/blu_ray_drm_cracked- (visited 17 June 2007)

[KK02]Larry Korba, Steve Kenny – Towards meeting the privacy challenge: adapting CS-9 Workshop DRM 2002 Springer ISBN 3-540-40410-4

[KK04] Kris Kaspersky – CD cracking uncovered, Protection against unsanctioned CD copying – 2004 A List LLC – ISBN 1-931769-33-8

[LI00] D Lie, C Thekkath, M Mitchell, P Lincoln, D Bohen – Architectural support for copy and tamper resistant software – Proceedings of the ninth International conference on architectural support for programming languages and operating systems – ACM -2000

[LA90] Lucasarts – the secret of monkey island -1990 http://www.mobygames.com/game/secret-of-monkey-island (visited 2 June 2007)

[MA07] Macrovision –http://www.macrovision.com – makers of the Activemark system. http://www.macrovision.com/solutions/distribution_commerce/game_publishers_portals/game_access_control.htm (visited 12 July 2007)

[MC07] http://www.mod-chip.com/ (visited 12 July 2007)

[MS02]Mark Stamp – digital rights management: the technology behind the hype, Cupertino, CA http://home.earthlink.net/~mstamp1/papers/DRMpaper.pdf (visited 4 July 2007)

[NS02] New scientist – Philips says copy-protected CDs have no future -Vol 2324 – 5th Jan 2002
http://www.newscientist.com/article.ns?id=dn1783 (visited august 2007)

[NV06a] National vulnerability database – Vulnerability summary CVE-2006-0858, star force vulnerability. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-0858 (visited July 2007)

[NV06b] National vulnerability database – Vulnerability summary CVE-2006-1197, safe disk vulnerability. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-1197 (visited July 2007)

[PB02] Peter Biddle - The darknet and the future of content protection digital rights management ACM CCS-9 workshop DRM 2002 ISBN 3-540-40410-4 Springer

[QL03] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard – Digital Rights management for content Distribution- Australasian Information security workshop 2003, Conferences in research and practice in Information technology , Vol 21

[RI01]Renato Iannella – Digital Rights Management Architectures -D-LIB Magazine Vol 7 no 6 – June 2001 – ISSN 1082-9873

[RL07] release log - Tomb Raider Anniversary-R55 – 2007
http://www.rlslog.net/tomb-raider-anniversary-r55/ (visited 12 June 07)

[ST07] http://www.steampowered.com/ (visited 3 July 2007)

[TM84] T Maude and D Maude – Hardware protection against software piracy – communications of the ACM 27 1984

[TT07] – Top ten game cop software reviews - http://game-copy-software-review.toptenreviews.com/ - (visited 1 august 2007)

[TR07] Trusted computing Group home –trusted computing group- http://www.trustedcomputinggroup.org/home - (visited 17 June 2007)

[VA07] Valve - http://www.valvesoftware.com/ (visited 2 July 2007)

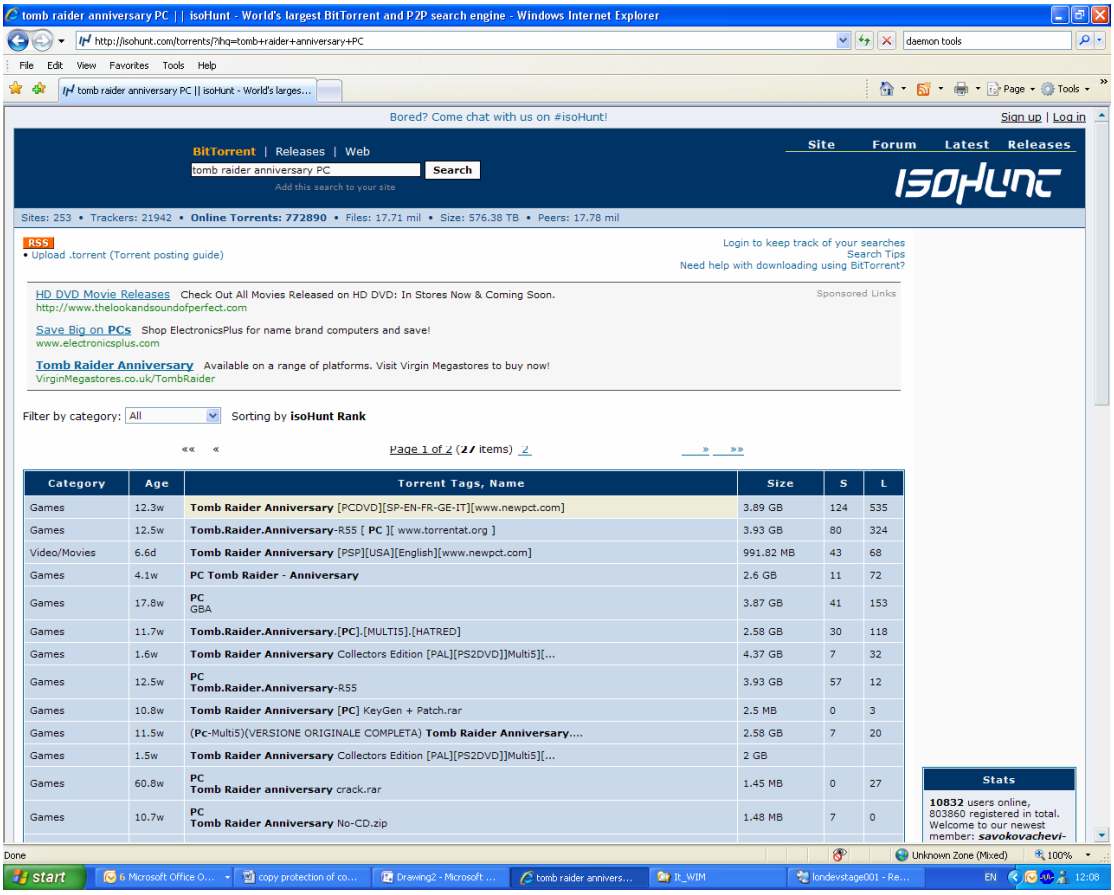
Appendix 1

Searching for a pirated version of tomb raider anniversary

Steps 1 – Find a bit torrent search or P2P search site

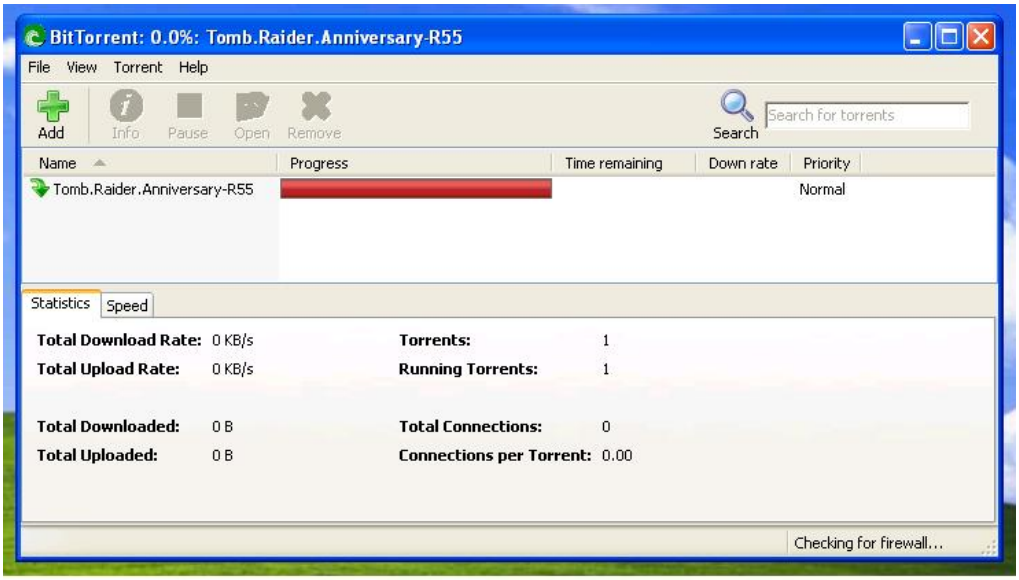
Google will find a number of search sites. One of the largest search engines was selected called ISOHunt.

Step 2 – search for tomb raider anniversary on ISOHunt

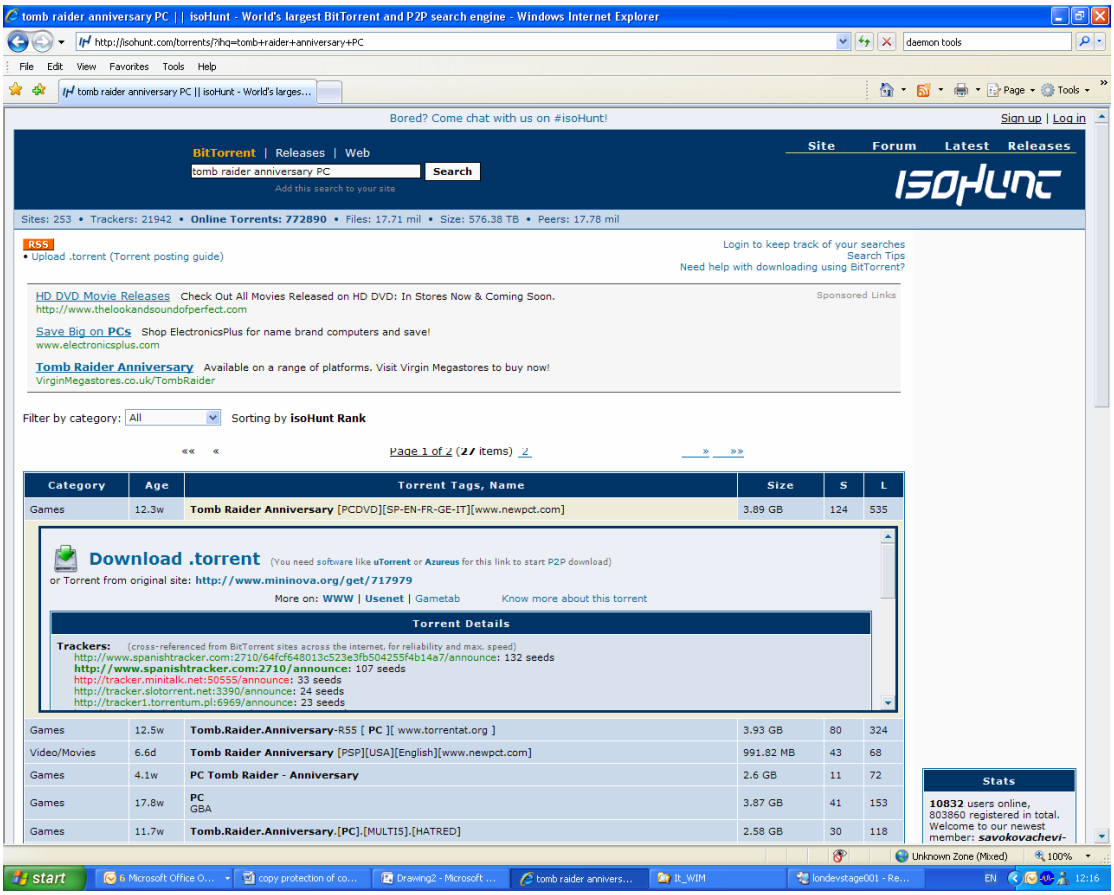


A search was conducted for Tomb raider Anniversary and a number of ISO images were found. The top one was selected.

Step 3 - A Client known as Bittorrent was installed on the PC.



Step 4 – Start the client downloading the ISO image



Clicking on the link will automatically send the relevant information to the client and downloading will start.

Step 5 – Unpack the ISO image and install on the hard drive and play the game.